DOCID: 4165384

~~TOP SECRET//COMINT//NOFORN//~~

SECURITY CLASSIFICATION

NSA STAFF PROCESSING FORM

TO	EXREG CONTROL NUMBER	KCC CONTROL NUMBER
DIRECTOR	92992	IG-10401-04

THRU	ACTION	EXREG SUSPENSE
D/DIR _____, D SECRETARIAT _____	☐ APPROVAL	
SUBJECT	☒ SIGNATURE	KCC SUSPENSE
(U//~~FOUO~~) Quarterly Report to the Intelligence Oversight Board on NSA Activities—Third Quarter FY04	☐ INFORMATION	ELEMENT SUSPENSE

DISTRIBUTION

SUMMARY

PURPOSE: (U//~~FOUO~~) To forward to the Intelligence Oversight Board (IOB) of the President's Foreign Intelligence Advisory Board, via the Assistant to the Secretary of Defense for Intelligence Oversight (ATSD(IO)), NSA's quarterly report on its intelligence activities.

BACKGROUND: (U//~~FOUO~~) Executive Order 12333 and Executive Order 12863 require Intelligence Community agency heads and Intelligence Community General Counsels and Inspectors General, respectively, to report to the IOB on a quarterly basis concerning intelligence activities that they have reason to believe may be unlawful or contrary to Executive Order or Presidential Directive. The enclosed memorandum covers all reportable activities known to the Inspector General and General Counsel. Per PIOB letter of 6 August 1982, Agency heads are responsible for reporting separately any additional reportable activities known to them, unless the President has specifically instructed that the Board is not to be informed. The Director's signature signifies that no other activities that require reporting are known to him.

RECOMMENDATION: (U) Director sign the enclosed memorandum.

Approved for Release by NSA on 12-22-2014, FOIA Case # 70809 (Litigation)

This document may be declassified
and marked "UNCLASSIFIED//~~For Official Use Only~~"
upon removal of enclosure(s)

(b)(3)-P.L. 86-36

COORDINATION/APPROVAL

OFFICE	NAME AND DATE	SECURE PHONE	OFFICE	NAME AND DATE	SECURE PHONE
GC	Robert L. Deitz	5548s	DoJ	9/10	963-3521
AGC(O)		3121s			
IG	Joel F. Brenner	3544s			
D/IG		3544s			
AIG(IO)		3544			

ORIGINATOR	ORG.	PHONE (Secure)	DATE PREPARED
	D11	963-2984	30 August 2004

FORM A6796 FEB 94
NSN: 7540-FM-001-5465

DERIVED FROM: NSA/CSSM 123-2
DATED: 24 February 1998
DECLASSIFY ON: X1

SECURITY CLASSIFICATION
~~TOP SECRET//COMINT//NOFORN//X1~~

~~TOP SECRET//COMINT//NOFORN//X1~~

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

13 September 2004

MEMORANDUM FOR THE CHAIRMAN, INTELLIGENCE OVERSIGHT BOARD

THRU: Assistant to the Secretary of Defense (Intelligence Oversight)

SUBJECT: (U//~~FOUO~~) Report to the Intelligence Oversight Board on NSA Activities - INFORMATION MEMORANDUM

(U//~~FOUO~~) Except as previously reported to you or the President, or otherwise stated in the enclosure, we have no reason to believe that any intelligence activities of the National Security Agency during the quarter ending 30 June 2004 were unlawful or contrary to Executive Order or Presidential Directive, and thus required to be reported pursuant to Section 1.7.(d) of Executive Order 12333.

(U//~~FOUO~~) The Inspector General and the General Counsel continue to exercise oversight of Agency activities by means of inspections, surveys, training, review of directives and guidelines, and advice and counsel. These activities and other data requested by the Board or members of the staff of the Assistant to the Secretary of Defense (Intelligence Oversight) are described in the enclosure.

JOEL F. BRENNER
Inspector General

ROBERT L. DEITZ
General Counsel

(U//~~FOUO~~) I concur in the report of the Inspector General and the General Counsel and hereby make it our combined report.

MICHAEL V. HAYDEN
Lieutenant General, USAF
Director, NSA/Chief, CSS

Encl:
Quarterly Report

This Document May Be Declassified and Marked "UNCLASSIFIED//~~FOR OFFICIAL USE ONLY~~" upon removal of enclosure(s).

DERIVED FROM: NSA/CSSM 123-2
Dated: 24 February 1998
Declassify on: X1

1. (U) INSPECTOR GENERAL ACTIVITIES

a. ~~(C//SI)~~ During this quarter, the Office of Inspector General (OIG) reviewed various intelligence activities of the National Security Agency/Central Security Service (NSA/CSS) to determine whether they were conducted in accordance with applicable statutes, Executive Orders (E.O.s), Attorney General procedures, and DoD and internal directives. With few exceptions, the issues presented were routine and indicated that the operating elements understand the restrictions on NSA/CSS activities.

b. ~~(S//SI)~~ The NSA OIG completed an inquiry (see our report dated 17 March 2004) into an instance of SIGINT Collection against a U.S. Person abroad without Attorney General authorization [redacted] While conducting our inquiry into this mishap, we encountered strong indications of shortcomings in the control environment that allowed this incident to occur and go undetected for almost six months. Corrective action has been directed and will be monitored through completion.

(b)(1)
(b)(3)-P.L. 86-36

c. ~~(S//SI//NF)~~ Two more individuals assigned to the [redacted] (see our quarterly reports of 18 September 2003 and 9 June 2004) have admitted misusing the U.S. SIGINT system by conducting unauthorized electronic surveillance of U.S. and non-U.S. persons abroad. The unauthorized surveillances were conducted for no legitimate foreign intelligence purpose.

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-50 USC 3024(i)

~~(S//SI//NF)~~ In response to these incidents the Director NSA and [redacted] issued a joint message to the [redacted] warning them of the consequences of misconduct of that type. A copy of the DIRNSA/ [redacted] message, together with amplifying remarks from the Director and Deputy Director of [redacted] are attached as Enclosure 1.

(b)(3)-P.L. 86-36

d. (U//~~FOUO~~) Along with inspectors from [redacted] the NSA OIG completed a joint inspection of [redacted] The joint inspection report notes that the site's intelligence oversight program is weak in training and documentation procedures. The inspection team noted that annual refresher training, which is accomplished by online posting of required reading material, is inconsistent and lacks documentation. A revisit to [redacted] by the Joint Inspectors General will be scheduled for next year.

2. (U) GENERAL COUNSEL ACTIVITIES

~~(C//SI)~~ The NSA Office of General Counsel (OGC) reviewed various intelligence activities of the NSA/CSS to determine whether they were conducted in accordance with applicable statutes, E.O.s, Attorney General procedures, and DoD and internal directives. The OGC advised Agency elements on a number of questions, including the collection and dissemination of communications of or concerning U.S. persons; the reporting of possible violations of federal criminal law contained in SIGINT product; the testing of electronic equipment; and the applicability of the Foreign Intelligence Surveillance Act (FISA). With few exceptions, the issues presented were routine and indicated that the operating elements understand the restrictions on NSA/CSS activities. The OGC did not file any reports with the Intelligence Oversight Board during this quarter.

3. (U) SIGINT ACTIVITIES

a. ~~(S//SI)~~ Collection Against U.S. Persons

(1) (U) Intentional

a. ~~(S//SI)~~ During this quarter, the Director of the National Security Agency (DIRNSA) granted approval for consensual collection against [ ] persons. DIRNSA-approved consensual collection against [ ] U.S. persons was routinely terminated this quarter.

(b)(1)
(b)(3)-P.L. 86-36

b. (S//SI) The Attorney General (AG) granted authority to collect the communications of [ ] U.S. persons during this quarter.

(2) (U) Unintentional

a. ~~(S//SI)~~ [ ] communications were inadvertently collected from a [ ] in which the called number was a U.S. number. Once noticed, [ ] were immediately deleted. The system is now undergoing testing to determine the reason for the collection of [ ]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

b. ~~(TS//SI)~~ An NSA integree to [ ] discovered during [ ] yrov, that a tasked [ ] was associated with [ ] turned out to be used by [ ]-based subscriber [ ], which handles [ ] business. Research into [ ] revealed he is a U.S. Citizen [ ]

(b)(1)
(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

. Upon discovering that is a U.S. Citizen, the NSA integree stopped working the traffic, As of the date of this report,

c. ~~(TS//SI)~~ the reports had been issued based on the collection. when research revealed that was an employee of the U.S. , the ceased collection and processing of communications between the and the U.S. person. As the intercepted communications contained significant foreign intelligence, the requested, pursuant to section 5.4 of USSID 18, a destruction waiver for the communications used as a basis for the SIGINT product. The request was approved by DIRNSA The has deleted all communications not relevant to the destruction waiver request and has taken steps to

d. ~~(S//SI//NF)~~ This quarter, unintentional retrievals using the raw traffic files resulted in incidents against U.S. persons overseas. All incidents were reported to responsible oversight officials and corrective actions were taken. All unauthorized traffic collected has been destroyed.

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36

b. (U//~~FOUO~~) Dissemination of U.S. Identities

(1) (U) Intentional

(b)(1)
(b)(3)-P.L. 86-36

~~(S//SI)~~ In accordance with section 7 of USSID 18, U.S. identities were disseminated times during this quarter. The following table shows the justification and the number of instances of dissemination:
In the "Unmasked by Analyst" column, the U.S. identity was revealed in a serialized end product; in the "Unmasked at User Request" column, a U.S. identity was released to a user at the user's request.

JUSTIFICATION	Unmasked by Analyst	Unmasked at User Request	TOTAL
7.2.c Necessary			
7.2.c.1 Foreign Official			
7.2.c.3 International Narcotics			
7.2.c.4 Criminal Activity			
7.2.c.7 U.S. Government Official			
TOTAL			

(b)(1)
(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

(b)(3)-P.L. 86-36
(b)(3)-18 USC 798
(b)(3)-50 USC 3024(i)

(2) (U) Unintentional

a. ~~(TS//SI)~~ The [redacted] had one incident of unintentional dissemination of a U.S. identity. [redacted] the [redacted] [redacted] A subsequent phone call to the same [redacted] official ensured the identity had not been further disseminated and that no action would be taken until the information was disseminated through proper channels. A limited distribution, special series report used to disseminate counterintelligence information was subsequently issued.

b. ~~(S//SI)~~ During this quarter, SID canceled [redacted] SIGINT products because they contained the identities of U.S. persons, organizations, or entities; those products that contained information derived from communications of U.S. persons were not reissued.

(b)(1)
(b)(3)-P.L. 86-36

c. ~~(TS//SI)~~ [redacted] released a total of [redacted] reports containing the identities of U.S. Persons or based on the communications of persons later identified as U.S. Persons. In all instances, [redacted] cancelled the reports, which were either not reissued or were reissued with the proper minimization.

(3) (U) Raw Traffic Dissemination Outside the SIGINT Production Chain

a. ~~(TS//SI)~~ As reported in the first quarter, raw SIGINT data was removed from the [redacted] classified website, which is available to both

(b)(3)-P.L. 86-36

(b)(1)
(b)(3)-P.L. 86-36

those personnel who are part of the SIGINT production chain and those who are not. The electronic and hard copy data has been destroyed. On 15 January 2004, [redacted] Intelligence Oversight Officer provided follow-up training to all persons involved in this incident.

b. ~~(TS//SI)~~ [redacted] (b)(3)-P.L. 86-36 [redacted] were given access to SIGINT information before their clearances were properly vetted. The pilot program's oversight manager and coordinator were informed of the deficiency and policy requirements. A database of clearance status was created to lessen the likelihood of future access violations.

c. ~~(S//SI)~~ As part of various agreements with other government agencies, non-SIGINT production elements of the NSA/CSS, or government contractors, non-SID personnel are granted access to unevaluated, unminimized SIGINT data. Many of these individuals are integrated into SID offices, while others provide essential enabling work (such as research) in their own spaces. The SID ensures that the personnel are trained by the OGC on NSA's legal restrictions and on proper handling and dissemination of SIGINT data prior to receiving access to raw data. Personnel working in or with SID during this quarter included representatives of the [redacted] (b)(3)-P.L. 86-36

[redacted]

4. (U) OTHER ACTIVITIES

(b)(1)
(b)(3)-P.L. 86-36

(U//FOUO) FISA Incidents

a. ~~(TS//SI)~~ [redacted] he [redacted] OGA (b)(7)(E) [redacted] that NSA was not authorized to collect. A [redacted] collection manager found the error [redacted] All of the files have been purged from NSA systems, and no reporting was done based on the unauthorized collection. As this error occurred because [redacted] failed to follow standard procedures to [redacted] was reminded of the importance of following standard operating procedures that ensure that [redacted] personnel will continue to perform periodic spot checks of forwarded data to guard against a repeat incident.

(b)(3)-P.L. 86-36

b. ~~(TS//SI//NF)~~ [redacted] (b)(1) OGA (b)(3) (b)(7)(E)

[redacted]

~~(TS//SI//NF)~~ [redacted]

[redacted]

(U) Assistance to Law Enforcement

~~(S//SI)~~ During this quarter, the SID responded to requests for technical assistance from law enforcement, including requests from [redacted] (b)(1) (b)(3)-P.L. 86-36 [redacted] Assistance included [redacted]

(U) Working Aids

(U//~~FOUO~~) The SID maintains "U.S. Identities in SIGINT" and a matrix of blanket reporting waivers on its web page for use by all NSA/CSS analysts. The E.O., NSA/CSS Policy 1-23, DoD Regulation 5240.1-R, and USSID 18 are also available on-line. Several offices in SID maintain files to be used to prevent targeting of U.S. persons.

(U) Intelligence Oversight Training

(U//~~FOUO~~) During this quarter an intelligence oversight specialist from the SID Office of Oversight and Compliance provided on-site training to military, civilian, and contractor personnel assigned to [redacted] (b)(3)-P.L. 86-36

[redacted] The NSA/CSS Office of General Counsel provided additional training to the [redacted] via video-teleconferencing. The training included Intelligence Oversight, E.O. 12333, USSID 9 and USSID 18, DOD Regulation 5240.1-R, NSA/CSS Policy 1-23, [redacted]

(b)(3)-P.L. 86-36

DOCID: 4165384

[redacted] (CIV-NSA) D11

From: [redacted]@nsa
Sent: Tuesday, August 24, 2004 3:26 PM
To: [redacted]@nsa
Subject: (U) PLEASE READ

(b)(3)-P.L. 86-36

Classification: ~~SECRET//COMINT//NOFORN//X1~~

DRV FM: Class. Guide 356-01
DATED: 3 July 2001
DECLON: X1

All, please read the note I received from Lt. Gen. Hayden and [redacted] this morning and then read [redacted] and my comments below it.

---------- Forwarded by [redacted] HQS on 08/24/2004 12:59 PM

"Hayden, Michael V. (MIL-USAF) D" <mvhayde@nsa> on 08/24/2004 08:33:47 AM

Please respond to mvhayde@nsa

To: [redacted]
cc: [redacted] "Black, William B (CIV-NSA) D" <wbblack@nsa>, [redacted]
Subject: (U) CA sends for DIR: Message from DIRNSA and [redacted] to [redacted] re Misuse of SIGINT systems

Classification: ~~SECRET//COMINT//NOFORN//X1~~

[redacted]

The enclosed message was coordinated with [redacted] to go out jointly from [redacted] and Gen Hayden. It is my understanding that you will disseminate on their behalf. Please let me know if you have any questions. Thanks!

(b)(3)-P.L. 86-36

[redacted]

[redacted]
Civilian Assistant to the Director
963-3111

> ~~(S//SI//NF)~~ In less than one year, three [redacted]

(b)(1)
(b)(3)-P.L. 86-36

> employees have admitted misusing the United States SIGINT System to
> conduct unauthorized electronic surveillances of both U.S. and non-U.S.
> persons abroad. These unauthorized surveillances were conducted for no
> legitimate foreign intelligence purpose. We are required to report these
> incidents to the Department of Justice for possible prosecution. Please
> inform your employees in the strongest terms that we will not tolerate
> misconduct of this kind, which may be punishable by recall from assignment
> and removal from [redacted] by separation from employment, and in the case of a
> criminal conviction, by fine and/or imprisonment.
>
>
>

(b)(3)-P.L. 86-36
(b)(1)

DRV FM: NSA/CSS Manual 123-2
Dated: 24 Feb 98
DECL ON: X1

Classification: ~~SECRET//COMINT//NOFORN//X1~~

Three of our colleagues have violated the trust we have placed in them. The use of our collection systems or any other government equipment for personal purposes is unacceptable under any circumstances. Although not referred to in this e-mail, failure to report foreign national contacts, failure to provide accurate financial accounting, failure to file accurate Time & Attendance reports, failure to pay Government credit card balances in a timely manner, etc. remain troubling issues among the [redacted] workforce and are also subject to severe penalties. In order to successfully execute our mission, all of you are given great latitude to meet your responsibilities. With this responsibility comes the accountability to remain within the rules, regulations and laws that apply. Failure to do so is a serious matter that will result in dire consequences as noted in the above e-mail. It is our responsibility to fully understand the rules, regulations and laws under which we operate. Our failure to understand these are not an acceptable defense. Know the rules - follow the rules. If you don't know or are unsure - ask. If you are considering violating the rules - don't. If you have violated the rules - tell us now.

(b)(3)-P.L. 86-36
(b)(1)

Unfortunately, these three individuals' actions coupled with other recent lapses of good judgement by a few of our [redacted] colleagues has resulted in increased scrutiny of all of us in [redacted] This increased scrutiny will continue until such time as we demonstrate, over a long period of time, that we are all fully responsible intelligence community employees who know and follow the rules while executing good judgment in all we do. [redacted] sent two e-mails some time ago stating that we have come too far to risk losing it due to our poor decisions while executing our mission. Likewise, I have spoken to a number of you here at Headquarters or in the field on my TDYs about the same thing. It remains true today and this e-mail from Lt. Gen. Hayden and [redacted] document a sad chapter in our proud history. In spite of this, we are still the premiere intelligence collection and reporting organization in the Intelligence Community. Everyday we make significant and timely contributions to the needs

(b)(3)-P.L. 86-36

of our country under often very difficult conditions. Everyday we make thousands of successful decisions that effect the security and safety of our country. Everyday the vast majority of us in [redacted] demonstrate integrity in our actions and are conscientious in doing our job within the parameters set for us. Everyday you make me proud to be a member of this organization and be given the opportunity to lead you. We cannot and should not tolerate illegal or inappropriate actions in our workforce - it detracts from all the good that we do and taints us by association. I ask for your increased attention to the rules, regulations and laws that we must follow. It is important for each of us to always conduct ourselves in a manner that is a model for others and beyond reproach.

(b)(1)
(b)(3)-P.L. 86-36

If you have questions or comments, please contact [redacted] or me.

(b)(3)-P.L. 86-36

Classification: ~~SECRET//COMINT//NOFORN//~~